

Numerical evidence for bound secrecy from two-way post-processing in quantum key distribution

Sumeet Khatri and Norbert Lütkenhaus

Institute for Quantum Computing and the Department of Physics and Astronomy, University of Waterloo, Waterloo, ON
(Dated: December 23, 2016)

Bound secret information is classical information that contains secrecy but from which secrecy cannot be extracted. The existence of bound secrecy has been conjectured but is currently unproven, and in this work we provide analytical and numerical evidence for its existence. Specifically, we consider two-way post-processing protocols in prepare-and-measure quantum key distribution based on the well-known six-state signal states. In terms of the quantum bit-error rate Q of the classical data, such protocols currently exist for $Q < \frac{5-\sqrt{5}}{10} \approx 27.6\%$. On the other hand, for $Q \geq \frac{1}{3}$ no such protocol can exist as the observed data is compatible with an intercept-resend attack. This leaves the interesting question of whether successful protocols exist in the interval $\frac{5-\sqrt{5}}{10} \leq Q < \frac{1}{3}$.

Previous work has shown that a necessary condition for the existence of two-way post-processing protocols for distilling secret key is breaking the symmetric extendability of the underlying quantum state shared by Alice and Bob. Using this result, it has been proven that symmetric extendability can be broken up to the 27.6% lower bound using the advantage distillation protocol. In this work, we first show that to break symmetric extendability it is sufficient to consider a generalized form of advantage distillation consisting of one round of post-selection by Bob on a block of his data. We then provide evidence that such generalized protocols cannot break symmetric extendability beyond 27.6%. We thus have evidence to believe that 27.6% is an upper bound on two-way post-processing and that the interval $\frac{5-\sqrt{5}}{10} \leq Q < \frac{1}{3}$ is a domain of bound secrecy.

I. INTRODUCTION

When considering prepare-and-measure-based (PM-based) quantum key distribution (QKD) protocols, to what extent can an eavesdropper tamper with the signals being sent by the sender (Alice) to the receiver (Bob) before classical post-processing protocols on the resulting measurement data cannot distill a secret key? More generally, which bipartite probability distributions between Alice and Bob contain secret bits that can be distilled into a secret key by some classical protocol?

Suppose Alice and Bob's data is given by measurement of many copies of a given quantum state ρ^{AB} . If ρ^{AB} is separable, then it is known that an intercept-resend attack exists and therefore no classical post-processing protocol can distill a secret key [1]. If ρ^{AB} is *symmetrically extendable to a copy of B*, then there exists a tripartite extension $\rho^{ABB'}$ of ρ^{AB} such that $\rho^{AB'} = \rho^{AB}$ [2]. In this situation, it is known that no one-way protocol involving communication from Alice to Bob can be used to distill a secret key because the system B' is effectively a copy of B and could belong to an eavesdropper (Eve), meaning that from Alice's point of view Bob and Eve are symmetric [3].

In this paper, we assume that Alice and Bob share many copies of the state $\rho_Q^{AB} = (1 - 2Q)|\Phi^+\rangle\langle\Phi^+| + \frac{Q}{2}\mathbb{1}_{AB}$, where $Q \in [0, \frac{1}{2}]$ is the quantum bit-error rate (QBER) and $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0,0\rangle + |1,1\rangle)$. They obtain their classical data by local measurement of each state in the standard basis $\{|0\rangle, |1\rangle\}$. This situation arises in PM-based six-state QKD protocols [4]. Since such protocols are tomographically complete, under a collective attack and in the infinite key limit, Alice and Bob can verify

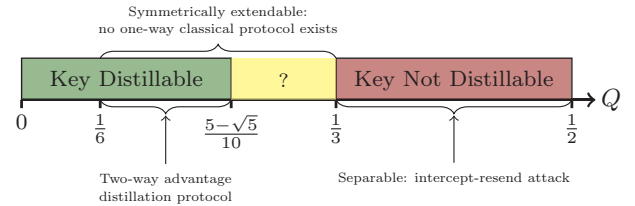


FIG. 1. Key distillability as a function of the QBER Q characterizing the quantum state ρ_Q^{AB} from which Alice and Bob obtain their classical data by measurement in the standard basis. We are interested in whether secret key can be distilled in the *gap*, that is, the yellow region.

that they indeed hold many copies of the state ρ_Q^{AB} [5]. As indicated in Figure 1, it is known that ρ_Q^{AB} is separable for $Q \geq \frac{1}{3}$ and symmetrically extendable for $Q \geq \frac{1}{6}$ [3]. By the arguments above, distilling secret key beyond $\frac{1}{6}$ would require a *two-way* classical post-processing protocol.

Gottesman and Lo [6] were the first to examine two-way classical post-processing protocols for PM-based QKD protocols. For the scenario we are considering here, they devised a two-way protocol that could distill secret key up to $Q = 26.4\%$. Chau [7] modified the Gottesman-Lo protocol and showed that secret key could be distilled up to $Q = \frac{5-\sqrt{5}}{10} \approx 27.6\%$, as shown in Figure 1. The protocols used by Gottesman-Lo and Chau were entanglement distillation protocols adapted to hold in a classical setting based on the Shor-Preskill proof of security of the BB84 protocol [8, 9]. The corresponding purely classical protocol is advantage distillation, which is a two-way classical protocol devised by Maurer [10] in

which Alice and Bob post-select on the repetition codes $\mathcal{R}_n = \{00 \cdots 00, 11 \cdots 11\}$ for some block length n . Acín [11] and Bae and Acín [12] showed explicitly that advantage distillation followed by error-correction and privacy amplification could distill secret key up to the Chau threshold and that beyond this threshold there exists an eavesdropping attack that causes advantage distillation to fail. To try to distill secret key beyond the Chau threshold, i.e., in the gap, Bae and Acín allowed Alice and Bob to perform noisy pre-processing before advantage distillation, and they even allowed Bob to perform coherent operations. Neither of these modifications could distill secret key beyond the Chau threshold.

Myhr et al. [13] then provided a new perspective on two-way protocols by shifting the goal from distilling secret key to *breaking symmetric extendability*. Specifically, they argued that if Alice and Bob's initial data corresponds to a symmetrically extendable state, then any successful two-way protocol must first transform this state to one that is not symmetrically extendable. This is due to the fact that any two-way protocol necessarily ends with a final round of one-way communication, which cannot be successful in distilling secret key unless Alice and Bob's correlations are not symmetrically extendable. They showed that all previous work pertaining to two-way protocols beyond $Q = \frac{1}{6}$ could be viewed in this way. In particular, they showed that advantage distillation breaks symmetric extendability up to the Chau threshold and that the existence of an eavesdropping attack beyond this threshold corresponds to the existence of a symmetric extension of the effective quantum state after advantage distillation. Bae and Acín's unsuccessful attempts to go beyond the Chau threshold can be understood similarly since local quantum operations, in particular noisy pre-processing and coherent operations by Bob, preserve symmetric extendability. To break symmetric extendability, Myhr et al. proved that it is sufficient to consider one announcement by Bob to Alice on a block of his data that can be described by one Kraus operator on the quantum states. To this end, Myhr in [5] considered a generalized form of advantage distillation in which Alice and Bob post-select on some pre-chosen linear error-correction code. He provided analytical and numerical evidence to suggest that such generalized protocols could not break symmetric extendability beyond the Chau threshold. Since only post-selection on linear codes was considered, his results left open the possibility that post-selection on *non-linear* codes might be able to break symmetric extendability beyond the Chau threshold.

We now consider post-selection on non-linear codes using the single-Kraus-operator formulation from Myhr et al. Specifically, in Section II we provide an explicit form for the Kraus operator, which allows us to obtain the effective quantum state after post-selection by Bob on *arbitrary* error-correction codes, i.e., both linear and non-linear codes. We describe the structure of the effective states and show that the search for codes breaking sym-

metric extendability beyond the Chau threshold can be reduced to the search over inequivalent codes. In Section III, we show analytically that repetition codes achieve the Chau threshold and numerically determine updated thresholds for inequivalent codes of small block lengths and number of codewords. From these results, we observe that repetition codes are optimal for each block length. In Section IV, we consider post-selection by Alice and Bob on the same code. From a random search on over 540,000 codes, we find that none are able to break symmetric extendability beyond the Chau threshold. We also introduce a procedure to construct a symmetric extension that works for 99% of the tested codes.

Our results lead us to the conjecture that repetition codes are optimal for each block length, meaning that there does *not* exist a code that can break symmetric extendability beyond the Chau threshold and therefore that secret key cannot be distilled in the gap. Since in the gap ρ_Q^{AB} is entangled, the corresponding classical data contains secret bits [14]. Therefore, if our conjecture is true, the data corresponding to the gap would contain *bound secrecy*, the classical analogue of bound entanglement in which classical data contains secret bits that cannot be extracted into a secret key by any protocol. The gap itself would then be an example of the separation between secrecy formation and secrecy extraction, the classical analogue of the separation between entanglement of formation and distillable entanglement. The existence of such a separation, as well as the existence of bound secrecy, has been conjectured with much evidence for its existence [14–19], but a proof has still not been found. Much of the prior evidence has focused on classical data arising from measurement of bound entangled states. Our results suggest that bound secrecy can be obtained even from measurement of quantum states with distillable entanglement.

II. FORMULATION OF THE PROBLEM

Even though PM-based protocols never actually involve bipartite entangled states, all such protocols can be modelled mathematically in terms of Alice preparing some pure bipartite entangled state $|\psi\rangle^{AB}$, measuring one half of it, and sending the other half to Bob, who then measures [20]. The resulting classical measurement data then corresponds to the quantum state $\rho^{AB} := (\mathbb{1}_A \otimes \Phi)(|\psi\rangle\langle\psi|^{AB})$ through the distribution $p_{AB}(i, j) = \text{Tr}[(A_i \otimes B_j)\rho^{AB}]$, where $\{A_i\}_i$, $\{B_j\}_j$ are Alice and Bob's measurement positive operator-valued measures (POVMs) and Φ is the channel through which Alice sends her signals to Bob and is assumed to be under Eve's control.

We are considering in this paper PM-based six-state QKD protocols in which Alice and Bob's classical data arise from individual measurement in the standard basis of several copies of the state $\rho_Q^{AB} = (1 - 2Q)|\Phi^+\rangle\langle\Phi^+| + \frac{Q}{2}\mathbb{1}_{AB}$. For $Q \geq \frac{1}{6}$, which is when this state is symmet-

rically extendable, no one-way classical post-processing protocol can distill a secret key, which means we must consider two-way protocols. We know from Myhr et al. [13] that any successful two-way protocol must transform the symmetrically extendable state ρ_Q^{AB} to an updated state that is not symmetrically extendable. They also proved that if we care only about breaking symmetric extendability (and not, say, about the value of the success probability and/or the secret-key rate), then it is sufficient to consider the symmetric extendability of the updated states corresponding to a single announcement by Bob on a block of his data of length n that can be described by one Kraus operator. If no such announcement can break symmetric extendability, then no general announcement will be able to, hence no two-way protocol will be able to distill a secret key. Since Bob's data is purely classical, his announcement can only be based on some partitioning of the n -bit strings $\{0, 1\}^n$. Suppose the set $\mathcal{C} = \{C_k\}_{k=0}^{m-1}$ of m distinct n -bit strings is one of the partitions. If Bob announces that his block of data is in \mathcal{C} , then the updated quantum state consistent with Alice and Bob's updated correlations, and the one from which key distillability after Bob's announcement can be determined, is

$$\rho_{Q,\mathcal{C}}^{A^n\tilde{B}} = (\mathbb{1}_{A^n} \otimes K_{\mathcal{C}})(\rho_Q^{AB})^{\otimes n}(\mathbb{1}_{A^n} \otimes K_{\mathcal{C}})^{\dagger}, \quad (1)$$

where

$$K_{\mathcal{C}} = \sum_{k=0}^{m-1} |k\rangle\langle C_k| \quad (2)$$

is the single Kraus operator corresponding to Bob's announcement. This is due to the fact that the conditional probability distribution of Alice and Bob's data given that Bob's data is in \mathcal{C} is the same as the probability distribution of Alice measuring the updated state (1) in the n -qubit standard basis and Bob measuring the updated state in the basis $\{|k\rangle\}_{k=0}^{m-1}$ corresponding to the elements of \mathcal{C} . Note that we get the same quantum state (1) if Bob merely performs *post-selection* on the set \mathcal{C} , that is, if Bob keeps his block of data if it is in \mathcal{C} and discards it otherwise, publicly announcing in each case what he does. In this way, we obtain a generalized form of the advantage distillation protocol.

Now, to determine the existence of two-way protocols, it is sufficient to consider the symmetric extendability of states of the form (1) [21]. The reason for this is that any general announcement scheme will be based on accepting the block of data if it is in some partition(s) of the n -bit strings. If announcing on each partition alone (for which the updated state is of the form (1)) cannot break symmetric extendability, neither can announcing on multiple partitions. We are thus interested in the symmetric extendability of the states (1). Specifically, we are interested in the *updated threshold* $Q_{\mathcal{C}}^*$, which we define as the value of the QBER beyond which the state is symmetrically extendable. (Note that without the Kraus operator the threshold is simply $\frac{1}{6}$ for all n .) The problem is

then to find a set \mathcal{C} with a threshold exceeding the Chau threshold, i.e., a set that breaks symmetric extendability in the gap.

Being a subset of the n -bit strings, the set \mathcal{C} can be thought of as a (classical) error-correction code with the elements of the set being the codewords. We will therefore throughout the rest of the paper call the set on which Bob post-selects a code and the elements of the set the codewords.

A. Structure of the Updated States

The updated state (1) can be written as

$$\rho_{Q,\mathcal{C}}^{A^n\tilde{B}} = \sum_{\alpha, \alpha' \in \{0,1\}^n} \sum_{k,k'=0}^{m-1} \left(\rho_{Q,\mathcal{C}}^{A^n\tilde{B}} \right)_{\alpha,k}^{\alpha',k'} |\alpha, k\rangle\langle\alpha', k'|,$$

where [22]

$$\begin{aligned} \left(\rho_{Q,\mathcal{C}}^{A^n\tilde{B}} \right)_{\alpha,k}^{\alpha',k'} &= \left(\frac{1-2Q}{2} \right)^{|\alpha \oplus \alpha'|} \left(\frac{Q}{2} \right)^{|\alpha \oplus C_k|} \\ &\times \left(\frac{1-Q}{2} \right)^{n-|\alpha \oplus \alpha'| - |\alpha \oplus C_k|} \\ &\times \delta_{\alpha \oplus C_k, \alpha' \oplus C_{k'}} \delta_{(\alpha \oplus C_k) \odot (\alpha \oplus \alpha'), \underline{0}^n}. \end{aligned} \quad (3)$$

Here, \oplus is the bit-wise XOR operation, \odot is the bit-wise AND operation, and $|\alpha|$ is the Hamming weight (number of ones) of the bit string α . The representation of the updated state in this manner depends on the ordering of \mathcal{C} and $\{0, 1\}^n$. A different ordering of these sets changes the updated state by local unitaries, which does not affect the corresponding threshold $Q_{\mathcal{C}}^*$ since symmetrically extendable states are preserved under local unitaries. We will therefore consider updated states corresponding to the same code to be equal if they differ only by local unitaries corresponding to a different ordering of the codewords.

The Kronecker delta $\delta_{\alpha \oplus C_k, \alpha' \oplus C_{k'}}$ in Eqn. (3) indicates that the elements of the updated state are non-zero if and only if $\alpha \oplus C_k = \alpha' \oplus C_{k'}$. This means that the (ordered) basis $\{|\alpha, k\rangle : \alpha \in \{0, 1\}^n, 0 \leq k \leq m-1\}$ can be changed to the new (ordered) basis $\bigcup_{\beta \in \{0, 1\}^n} \{|\alpha, k\rangle : \alpha \oplus C_k = \beta\}$ by a unitary V that leaves the updated state in a *block-diagonal* form,

$$V \rho_{Q,\mathcal{C}}^{A^n\tilde{B}} V^{\dagger} = \bigoplus_{\beta \in \{0, 1\}^n} M_{Q,\mathcal{C}}^{(\beta)}, \quad (4)$$

where $M_{Q,\mathcal{C}}^{(\beta)}$ are the blocks, each $m \times m$, with elements $\left(M_{Q,\mathcal{C}}^{(\beta)} \right)_k^k = \left(\rho_{Q,\mathcal{C}}^{A^n\tilde{B}} \right)_{\beta \oplus C_k, k}^{\beta \oplus C_k, k}$ for all $0 \leq k, k' \leq m-1$.

For a *direct sum* of codes $\mathcal{C}_1 = \{C_{1,k}\}_{k=0}^{m_1-1}$ of block length n_1 and $\mathcal{C}_2 = \{C_{2,k}\}_{k=0}^{m_2-1}$ of block length n_2 , the updated state has a tensor product structure in addition to the block diagonal structure. The direct sum is the

code $|\mathcal{C}_1|_{\mathcal{C}_2}| = \{C_{1,k}C_{2,\ell} : 0 \leq k \leq m_1 - 1, 0 \leq \ell \leq m_2 - 1\}$ with block length $n_1 + n_2$ and $m_1 m_2$ codewords [23]. In this case, it is straightforward to show [22] that the updated state is equal to

$$\rho_{Q,|\mathcal{C}_1|_{\mathcal{C}_2}|}^{A^{n_1+n_2}\tilde{B}} = \rho_{Q,\mathcal{C}_1}^{A^{n_1}\tilde{B}_1} \otimes \rho_{Q,\mathcal{C}_2}^{A^{n_2}\tilde{B}_2}. \quad (5)$$

The corresponding threshold is then equal to

$$Q_{|\mathcal{C}_1|_{\mathcal{C}_2}|}^* = \max\{Q_{\mathcal{C}_1}^*, Q_{\mathcal{C}_2}^*\} \quad (6)$$

since the state is symmetrically extendable if and only if each state in the tensor product is symmetrically extendable. Analogous results for the updated state and threshold hold for a direct sum of more than two codes, which is defined analogously to the direct sum of two codes.

B. Equivalent Codes

Two codes $\mathcal{C} = \{C_k\}_{k=0}^{m-1}$ and $\mathcal{D} = \{D_k\}_{k=0}^{m-1}$, each with block length n , are called *equivalent* if there exists a permutation π on n bits and $\alpha \in \{0,1\}^n$ such that $\pi(\mathcal{D}) \oplus \alpha := \{\pi(D_k) \oplus \alpha : 0 \leq k \leq m-1\} = \mathcal{C}$ [23]. If \mathcal{C} and \mathcal{D} are equivalent, then [22]

$$\rho_{Q,\mathcal{C}}^{A^n\tilde{B}} = \rho_{Q,\mathcal{D}}^{A^n\tilde{B}} \quad \forall 0 \leq Q \leq \frac{1}{2}, \quad (7)$$

which means that $Q_{\mathcal{C}}^* = Q_{\mathcal{D}}^*$. Therefore, for any given block length n and number of codewords m , to find a code exceeding the Chau threshold we need only search the inequivalent codes.

We can remove from the set of inequivalent codes those that contain constant columns when written as a matrix with each codeword forming a row. This is due to the fact that any such code is equivalent to a code of the form $\mathcal{C}' = \{\beta C_k\}_{k=0}^{m-1} = |\{\beta\}|\mathcal{C}|$ for some $\beta \in \{0,1\}^x$, and by Eqn. (5) it holds that

$$\rho_{Q,\mathcal{C}'}^{A^{n+x}\tilde{B}} = \rho_{Q,\{\beta\}}^{A^x\tilde{B}_1} \otimes \rho_{Q,\mathcal{C}}^{A^n\tilde{B}_2}. \quad (8)$$

Since $\rho_{Q,\{\beta\}}^{A^x\tilde{B}_1}$ is symmetrically extendable for all $Q \in [0, \frac{1}{2}]$ (\tilde{B}_1 is one-dimensional), it holds that $Q_{\mathcal{C}'}^* = Q_{\mathcal{C}}^*$. In other words, removing the constant columns gives a code without constant columns (and with smaller block length) that has the same threshold as the original code.

For any given (n, m) class, we can thus take all codes without constant columns and run through all pairs of permutations and bit strings to determine the number of inequivalent codes. For small (n, m) classes, we obtain the numbers in Table I. Notably, with two codewords, the repetition code $\mathcal{R}_n = \{00 \cdots 00, 11 \cdots 11\}$ is the only inequivalent code without constant columns for all $n \geq 2$. Determining the number of inequivalent codes for higher (n, m) classes becomes very rapidly lengthy since the number of permutations is $n!$ and the number of bit strings is 2^n , resulting in $n! \times 2^n$ pairs of permutations and bit strings over which to search.

$n \backslash m$	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	1	1												
3	1	2	5	3	3	1								
4	1	3	13	24	47	55	73	56	50	27	19	6	4	1
5	1	4	28	104	422
6	1	6	56
7	1	7
8	1	9

TABLE I. Number of inequivalent codes without constant columns for some small (n, m) classes. For each n , the largest m such that the code is non-trivial is $2^n - 1$. Numbers for the cells with a dot have not been calculated.

III. UPDATED THRESHOLDS

Our goal is to find a code such that the corresponding updated state (1) has a threshold in the gap of Figure 1. From the previous section, we know that it is sufficient to search over inequivalent codes without constant columns. In this section, we determine the threshold of the codes in many of the (n, m) classes for which the number of inequivalent codes without constant columns has been determined, as indicated in Table I, where n is the block length and m the number of codewords. First, in Section III A, we provide the analytical result that repetition codes, the only inequivalent code without constant columns containing two codewords, reproduce the Chau threshold and the known result from [13] that advantage distillation cannot break symmetric extendability in the gap. In fact, our result builds on that result from [13] since in that work they considered post-selection by Alice and Bob on repetition codes while we consider post-selection only by Bob. (We consider the less general case of Alice post-selecting on the same code as Bob in Section IV.) We then numerically determine the thresholds for other (n, m) classes in Section III B and describe trends in the thresholds that lead us to believe that repetition codes are optimal for each block length. In Section III C, we examine the best codes among the tested (n, m) classes and in Section III D we go through some areas for future work.

A. Repetition Codes

For the repetition codes $\mathcal{R}_n = \{00 \cdots 00, 11 \cdots 11\}$, it holds that for each $n \geq 1$ the threshold $Q_{\mathcal{R}_n}^*$ is the solution to

$$4Q^{2n} - 4Q^n(1 - Q)^n + (1 - 2Q)^{2n} = 0. \quad (9)$$

We provide a sketch of the proof of this fact in Appendix A, while the full proof can be found in [22].

The thresholds $Q_{\mathcal{R}_n}^*$ are plotted in Figure 2. They increase monotonically with n and appear to converge to the Chau threshold $\frac{5-\sqrt{5}}{10} \approx 27.6\%$ in the limit $n \rightarrow$

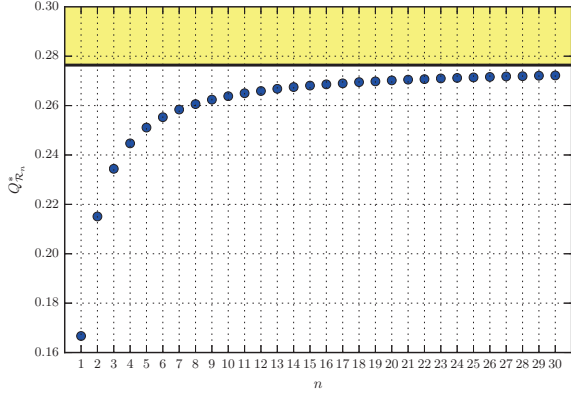


FIG. 2. Repetition code thresholds $Q_{\mathcal{R}_n}^*$ up to $n = 30$.

∞ . Indeed, it can be shown [22] that as n increases the thresholds approach

$$\tilde{Q}_{\mathcal{R}_n}^* := \frac{\left(4\left(\frac{1}{4}\right)^{\frac{1}{n}+1}\right) - \sqrt{\left(4\left(\frac{1}{4}\right)^{\frac{1}{n}+1}\right)^2 - 4\left(\frac{1}{4}\right)^{\frac{1}{n}}\left(4\left(\frac{1}{4}\right)^{\frac{1}{n}+1}\right)}}{2\left(4\left(\frac{1}{4}\right)^{\frac{1}{n}+1}\right)}. \quad (10)$$

Since $\lim_{n \rightarrow \infty} \tilde{Q}_{\mathcal{R}_n}^* = \frac{5-\sqrt{5}}{10}$, which is precisely the Chau threshold, it holds that the actual threshold approaches the Chau threshold as well. This reproduces the result from [13] that advantage distillation cannot break symmetric extendability beyond the Chau threshold, although, as mentioned earlier, we have considered post-selection only by Bob while in [13] post-selection by Alice as well was considered.

B. Numerical Determination of Thresholds for Arbitrary Codes

There are currently no known symmetric extendability results that allow us to determine the thresholds for codes other than repetition codes. Fortunately, we can still numerically determine the thresholds using the following semi-definite program (SDP) that can be used to determine the symmetric extendability of an arbitrary positive semi-definite operator P^{AB} :

$$\begin{aligned} \min. \quad & t \\ \text{subject to} \quad & R^{ABB'} + t\mathbb{1}^{ABB'} \geq 0, \\ & \text{Tr}_B[R^{ABB'}] = P^{AB}, \\ & \text{Tr}_{B'}[R^{ABB'}] = P^{AB}. \end{aligned} \quad (11)$$

When the minimum value $t_{\min}(P^{AB})$ of the objective function t is positive P^{AB} is not symmetrically extendable, and when $t_{\min}(P^{AB})$ is non-positive P^{AB} is symmetrically extendable, with the operator $R^{ABB'}$ achieving the minimum being a symmetric extension.

For the updated states (1), each code \mathcal{C} corresponds to the function $T_{\mathcal{C}} : [0, \frac{1}{2}] \rightarrow \mathbb{R}$ defined by

$$T_{\mathcal{C}}(Q) = t_{\min}(\rho_{Q,\mathcal{C}}^{A^n \bar{B}}). \quad (12)$$

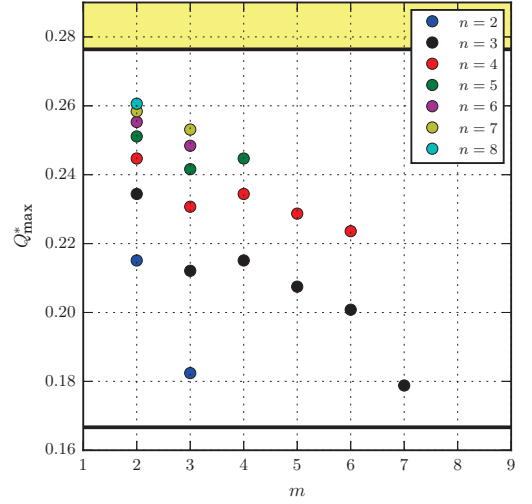


FIG. 3. The highest thresholds for some of the (n, m) classes from Table I.

The zero of $T_{\mathcal{C}}$ is then the threshold $Q_{\mathcal{C}}^*$. To obtain the threshold, we selected 200 points (evenly spaced) in the QBER interval $\mathcal{I} = [0.16, 0.33]$ and determined the zero of the curve-of-best-fit to the points $\{T_{\mathcal{C}}(Q) : Q \in \mathcal{I}\}$ corresponding to an estimate of the function $T_{\mathcal{C}}$. The points $T_{\mathcal{C}}(Q)$ were obtained by solving the SDP (11) in MATLAB using yalmip [24] with the solver SCS [25] to a precision of 10^{-10} . The best-fitting curve was obtained in MATLAB using a cubic spline model. This procedure leads to thresholds that are accurate to within 8.5×10^{-4} , which is the spacing between the points in the interval \mathcal{I} . For codes containing more than two codewords ($m > 2$), we applied this procedure to many of the (n, m) classes in Table I for which the number of inequivalent codes without constant columns is known. Specifically, for $m = 3$ we determined the thresholds up to $n = 7$, for $m = 4$ up to $n = 5$, for $m = 5$ and $m = 6$ up to $n = 4$, and for $m = 7$ up to $n = 3$. The highest threshold for each (n, m) class tested is plotted in Figure 3. Determining the threshold for higher (n, m) classes becomes increasingly time-consuming and resource-intensive since each code requires 200 SDPs and each SDP takes longer to complete, and requires more computer memory, as n and m increase and with it the number of optimization variables. As well, since the dimension of Alice's space is 2^n , memory limits can be quickly reached in just storing the updated state.

From the plot in Figure 3, we observe that for each block length n , the $(n, 2)$ class, which contains only the repetition code \mathcal{R}_n , has the highest threshold. For fixed n , as the number of codewords m increases beyond 2, the threshold tends to decrease. This suggests that repetition codes are optimal for any given block length and therefore that codes with a high number of codewords are unlikely to be helpful in obtaining a threshold exceeding the Chau threshold. In particular, we have a clear sign that non-linear codes are not necessarily better than linear codes

and that they are actually worse than linear codes in some cases since the $m = 3, 5, 6, 7$ codes are necessarily non-linear and their highest thresholds are less than the highest thresholds of the $m = 2$ and $m = 4$ codes, which are given by linear codes. (We will see that the best $m = 4$ codes are linear in the next subsection.) As well, for fixed m , the threshold increases with increasing n , with a clear indication, particularly for small m , that the thresholds are converging to the Chau threshold.

C. Codes with the Highest Threshold

Having seen that the repetition code appears optimal for each block length n , we now examine the best codes, i.e., the codes with the highest threshold, for each number of codewords m . Since for all block lengths the repetition code is the only inequivalent code without constant columns containing two codewords, it is the best code with two codewords. In the following, we write codes as a matrix in which each row of the matrix is a codeword.

With three codewords, the best codes are

$$\begin{bmatrix} 00 \\ 01 \\ 11 \end{bmatrix}, \begin{bmatrix} 000 \\ 011 \\ 111 \end{bmatrix}, \begin{bmatrix} 0000 \\ 0111 \\ 1111 \end{bmatrix}, \begin{bmatrix} 00000 \\ 01111 \\ 11111 \end{bmatrix}, \begin{bmatrix} 000000 \\ 011111 \\ 111111 \end{bmatrix}, \begin{bmatrix} 0000000 \\ 0111111 \\ 1111111 \end{bmatrix}. \quad (13)$$

There is a clear trend among these codes, so we conjecture that for all $n \geq 2$ the best three-codeword code is

$$\begin{bmatrix} 00 \dots 00 \\ 01 \dots 11 \\ 11 \dots 11 \end{bmatrix}.$$

With four codewords, the best codes are

$$\begin{bmatrix} 000 \\ 011 \\ 100 \\ 111 \end{bmatrix}, \begin{bmatrix} 0000 \\ 0111 \\ 1000 \\ 1111 \end{bmatrix}, \begin{bmatrix} 00000 \\ 01111 \\ 10000 \\ 11111 \end{bmatrix}. \quad (14)$$

Each of these codes is linear and equal to $|\mathcal{R}_1|\mathcal{R}_{n-1}|$, so that the threshold is equal to $Q_{\mathcal{R}_{n-1}}^*$. We conjecture therefore that for all $n \geq 3$ the best four-codeword code is $|\mathcal{R}_1|\mathcal{R}_{n-1}|$.

With five codewords, the best codes are

$$\begin{bmatrix} 000 \\ 001 \\ 011 \\ 100 \\ 111 \end{bmatrix}, \begin{bmatrix} 0000 \\ 0011 \\ 0111 \\ 1000 \\ 1111 \end{bmatrix}. \quad (15)$$

Both of these codes are of the form

$$\begin{bmatrix} 0 & | & 00 \dots 00 \\ 0 & | & 01 \dots 11 \\ 0 & | & 11 \dots 11 \\ \hline 1 & | & 00 \dots 00 \\ 1 & | & 11 \dots 11 \end{bmatrix}. \quad (16)$$

That is, the two codes are composed of the codewords of the conjectured best $(n-1, 3)$ code and the codewords of the repetition code \mathcal{R}_{n-1} . As well, the thresholds of the two codes are between the thresholds of the two smaller codes comprising them.

With six codewords, the best codes are

$$\begin{bmatrix} 000 \\ 001 \\ 010 \\ 011 \\ 100 \\ 111 \end{bmatrix}, \begin{bmatrix} 0000 \\ 0011 \\ 0101 \\ 0111 \\ 1000 \\ 1111 \end{bmatrix}. \quad (17)$$

Like the best five-codeword codes in Eqn. (15), these codes are of the form

$$\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ \hline 1 \\ 1 \end{bmatrix} \begin{array}{c} \mathcal{C} \\ \mathcal{R}_{n-1} \end{array} \quad (18)$$

for a $(n-1, 4)$ code \mathcal{C} . In Eqn. (15), \mathcal{C} is the best code in the $(n-1, 3)$ class, while in the best $(4, 6)$ code \mathcal{C} is *not* the best $(3, 4)$ codeword $|\mathcal{R}_1|\mathcal{R}_2|$. However, letting $\mathcal{C} = |\mathcal{R}_1|\mathcal{R}_2|$ gives a code that differs by only one codeword and has threshold that is the same as the threshold of that best code up to four decimal places. (For the best $(3, 6)$ code, \mathcal{C} is equal to all the two-bit strings, which is the only possibility since there are only four two-bit strings.)

For each number of codewords m , the best codes appear to form a sequence in which the block length is increased by one by adding some fixed column to the code. This is clear particularly for $m = 3$ and $m = 4$: for $m = 3$, adding the column $\begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$ to the best $(n, 3)$ code produces the best $(n+1, 3)$ code, while for $m = 4$ adding the column $\begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$ produces the best four-codeword code of the next block length. Increasing the block length in this way also increases the threshold, though the increase diminishes with increasing block length. These results are consistent with our results on repetition codes, in which adding the column $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ to \mathcal{R}_n produces \mathcal{R}_{n+1} , which has a higher threshold than \mathcal{R}_n . Just as the repetition code thresholds approach the Chau threshold in the limit $n \rightarrow \infty$, it appears from Figure 3 that the sequence of best three-codeword codes approaches the same threshold as $n \rightarrow \infty$. This leads us to believe that the best codes for each number of codewords will be a sequence of codes defined by successively adding some fixed column to the previous code in the sequence and that the thresholds of these codes will approach the Chau threshold.

D. Directions for Future Work

Based on our results from the previous subsections, we now go through some directions for future work. First, finding the best codes for higher (n, m) classes, particularly for the (n, m) classes in Table I for which the best codes have not yet been found, will help in developing a better understanding of the structure of the best codes. As alluded to near the end of the previous subsection, another potential area for future work is examining the effect on the threshold of making very small changes to codewords. See [22] for examples of codes differing by only one codeword that have very close thresholds.

Also at the end of the previous subsection, we made the observation that for the best codes examined in that subsection successively adding some fixed column to the best (n, m) code gives the best m -codeword code for higher block lengths. To see if this observation might generalize to the best codes for all m , we are interested in examining the effect on the threshold of adding columns to a code. Specifically, for a given (n, m) code \mathcal{C} , we are interested in the 2^m codes in the $(n+1, m)$ class obtained by adding each m -bit string as a column to \mathcal{C} . Note that the two codes obtained by adding a column and its complement (the string obtained by flipping each bit) are equivalent. Furthermore, as we know from Section II B, adding a constant column to a code does not change the threshold. This leaves at most $2^{m-1} - 1$ inequivalent codes without constant columns whose thresholds can be compared to that of \mathcal{C} to see which, if any, increases the threshold.

We are also interested in the following generalization of repetition codes that takes a (n, m) code \mathcal{C} and produces a $(n+1, 2m)$ code defined as

$$\left[\begin{array}{c|c} 0 & \\ \vdots & \\ 0 & \mathcal{C} \\ \hline 1 & \\ \vdots & \bar{\mathcal{C}} \\ 1 & \end{array} \right], \quad (19)$$

where $\bar{\mathcal{C}}$ is called the *complement* of \mathcal{C} and is composed of the complement of each codeword in \mathcal{C} . We call (19) the *complement extension* of \mathcal{C} . It is closed under taking the complement, in short *complement-closed*, since each codeword and its complement are contained in the code. Conversely, any complement-closed code is equivalent to the complement extension of some code. Complement-closed codes are a generalization of repetition codes that contain non-linear codes. An even broader generalization of repetition codes can be obtained by replacing $\bar{\mathcal{C}}$ with $\pi(\mathcal{C}) \oplus \alpha$, that is, with some code equivalent to \mathcal{C} . This extension, which we call the (π, α) *extension*, contains the complement extension as a special case when π is the identity permutation and $\alpha = 11 \cdots 11$. We are interested in whether the (π, α) extension can increase the threshold of the original code \mathcal{C} , particularly when

\mathcal{C} is the best code in a class containing an odd number of codewords. The reason for this is that for the best three-codeword codes (13) there exist multiple (π, α) extensions that increase the threshold. In fact, one of them is always the complement extension, though it does not always provide the highest increase in the threshold. If we can thus show that for all the best codes with an odd number of codewords there exists a (π, α) extension with a higher threshold, then we could restrict the search for codes exceeding the Chau threshold to those containing only an even number of codewords.

IV. POST-SELECTION BY ALICE

As mentioned in the previous section, one of the challenges in testing codes with larger block lengths is that the dimension of Alice's space in the updated states (1) is 2^n . This results in SDPs that take a very long time to complete and often exceed the computer's memory limits. One way to address these issues is to allow Alice to post-select on the same code as Bob, resulting in the updated states

$$\begin{aligned} & (K_{\mathcal{C}} \otimes K_{\mathcal{C}})(\rho_Q^{AB})^{\otimes n}(K_{\mathcal{C}} \otimes K_{\mathcal{C}})^{\dagger} \\ &= (K_{\mathcal{C}} \otimes \mathbb{1}_{\bar{\mathcal{B}}})\rho_{Q,\mathcal{C}}^{A^n \bar{B}}(K_{\mathcal{C}} \otimes \mathbb{1}_{\bar{\mathcal{B}}})^{\dagger}. \end{aligned} \quad (20)$$

This reduces the dimension of Alice's space to the same as Bob's and generally speeds up the SDP; however, it will not help to increase the threshold since the state (20) is symmetrically extendable whenever the state $\rho_{Q,\mathcal{C}}^{A^n \bar{B}}$ is symmetrically extendable. Since the converse of this statement is not necessarily true, post-selection by Alice might *decrease* the threshold. For the repetition codes, however, we find that this is not the case, that is, the thresholds with and without post-selection by Alice are the same for all block lengths; see Appendix A for a sketch of the proof. We have evidence to believe that the same might be true for the vast majority of codes, including the best codes from Section III C, though we have found codes for which the thresholds are clearly different; see Appendix B for some examples.

In this section, we first consider a class of codes generalizing the repetition codes for which we were able to analytically determine the thresholds under post-selection by Alice. We then describe a procedure to attempt a construction of a symmetric extension of any positive semi-definite operator that potentially avoids running the SDP (11). By randomly selecting codes with larger block lengths and applying this procedure to the states (20), we then examine symmetric extendability in the gap in the case of Alice post-selecting on the same code as Bob.

A. Simplex Codes

One natural way of generalizing repetition codes to more than two codewords is to consider codes in which

all pairs of distinct codewords are some fixed Hamming distance, say d , away from each other. Such codes are called *simplex codes* [23]. Unlike the linear repetition codes, however, simplex codes can be non-linear, which makes them of interest to us. Simplex codes $\mathcal{S}_{n,m,d}$ can be specified uniquely (up to equivalence and without constant columns) by three parameters: the block length n , the number of codewords m , and the constant Hamming distance d separating the codewords. When Alice and Bob post-select on the same simplex code, the state (20), that is,

$$(K_{\mathcal{S}_{n,m,d}} \otimes K_{\mathcal{S}_{n,m,d}})(\rho_Q^{AB})^{\otimes n}(K_{\mathcal{S}_{n,m,d}} \otimes K_{\mathcal{S}_{n,m,d}})^\dagger, \quad (21)$$

can be shown to be diagonal in the m -dimensional Bell basis $\{|\Phi_{k,\ell}\rangle\}_{a,b=0}^{m-1}$ defined by $|\Phi_{k,\ell}\rangle = (\mathbb{1}_{\mathbb{C}^m} \otimes X(k)Z(\ell))\frac{1}{\sqrt{m}}\sum_{j=0}^{m-1}|j,j\rangle$, where $X(k)$, $Z(\ell)$ are the generalized Pauli (also called discrete Weyl) operators [26]. The state has only three distinct eigenvalues and is of the form

$$\rho^{AB} = \sum_{k,\ell=0}^{m-1} x_{k,\ell} |\Phi_{k,\ell}\rangle \langle \Phi_{k,\ell}|, \quad (22)$$

$$x_{k,\ell} = \begin{cases} a & \text{if } k = \ell = 0, \\ b & \text{if } k = 0, \ell \geq 1, \\ \frac{1-a-(m-1)b}{m(m-1)} & \text{otherwise,} \end{cases}$$

where $a \geq b$ and $x := a + (m-1)b \leq 1$. It is known [27, Theorem 3] that such states are symmetrically extendable for all $m \geq 2$ if and only if

$$a - b \leq 2\sqrt{\frac{(1-x)(2x-1)}{m-1}} + \frac{m-2}{m-1}(1-x). \quad (23)$$

By determining the eigenvalues of the state (21) and substituting them into Eqn. (23), the resulting condition at equality gives the symmetric extendability threshold of the state (21). For any simplex code, we find (see [22] for details) that the threshold is never greater than the repetition code threshold for the same block length. In fact, as observed with the highest thresholds in Figure 3, for each block length the thresholds decrease as the number of codewords increases beyond two, which means that non-linear simplex codes are not better than the repetition codes for fixed block length. Furthermore, as the distance d increases, we find that the thresholds approach the repetition code thresholds. In fact, in the limit $d \rightarrow \infty$, the thresholds approach $\frac{5-\sqrt{5}}{10}$, the same as the repetition code thresholds. This means that simplex codes cannot break symmetric extendability in the gap, at least in the case of Alice post-selecting on the same code as Bob. This result also shows us that the repetition codes are not the only ones that can achieve the Chau threshold. While for repetition codes we were able to prove that the thresholds with and without post-selection by Alice are the same for all block lengths, the method of proof used in that case did not work for simplex codes

in general. Nevertheless, for some small simplex codes, we saw a difference between the thresholds on the order of 10^{-6} or less, which suggests that the thresholds might be the same.

B. Constructing a Symmetric Extension and Random Search Over Larger Codes

Though considering post-selection by Alice on the same code as Bob generally reduces the runtime of the SDP (11), to speed up the determination of symmetric extendability even further we developed a procedure to attempt a construction of a symmetric extension of the updated states (20). This procedure can also be used on the updated states (1) without post-selection by Alice (in fact, it can be used on any positive semi-definite operator), and is based on the following facts: every positive semi-definite operator P^{AB} is uniquely associated with a completely-positive (CP) map Φ from A to B (this is the Choi-Jamiolkowski correspondence) [26]; P^{AB} is symmetrically extendable if and only if Φ is *anti-degradable*, that is, if and only if there exists a *degrading channel* \mathcal{E} such that $\mathcal{E} \circ \Phi^c = \Phi$, where Φ^c is a CP map complementary to Φ [5]; if P^{AB} is symmetrically extendable, then $P^{ABB'} := (\mathbb{1}_{AB} \otimes \mathcal{E})(|\psi\rangle\langle\psi|^{ABE})$ is a symmetric extension, where $|\psi\rangle^{ABE}$ is a purification of P^{AB} corresponding to Φ^c and \mathcal{E} is a degrading channel from the definition of anti-degradability of Φ [22]. In the procedure, we assume that a fixed orthonormal product basis $\{|e_i\rangle^A \otimes |f_j\rangle^B \equiv |e_i, f_j\rangle^{AB}\}_{i,j}$ has been chosen in which to represent P^{AB} . The procedure is as follows.

1. Take $|\psi\rangle^{ABE_1E_2} = \text{vec}(\sqrt{P^{AB}})$ as a purification of P^{AB} , where the operation vec is defined in the basis $\{|e_i, f_j\rangle^{AB}\}_{i,j}$ as $\text{vec}(|e_i, f_j\rangle\langle e_{i'}, f_{j'}|) = |e_i, f_j\rangle \otimes |e_{i'}, f_{j'}\rangle$. This operation defines the purification space E as the tensor product $E_1 \otimes E_2$, where E_1 is spanned by $\{|e_i\rangle\}_i$ and has the same dimension as A and where E_2 is spanned by $\{|f_j\rangle\}_j$ and has the same dimension as B .
2. Use as ansatz a degrading map of the form $\mathcal{E} = \mathcal{N} \circ \text{Tr}_{E_2}$, where the map \mathcal{N} is defined by the condition that \mathcal{E} satisfies the definition of anti-degradability of Φ .
3. Since \mathcal{N} must also be a channel, check that it is CP and trace-preserving, which can be done, for example, using the Choi representation; see [22] for the details. If it is, then P^{AB} is symmetrically extendable, otherwise run the SDP (11).

With this procedure, we can potentially avoid running the SDP (11), thereby dramatically decreasing the amount of time it takes to determine symmetric extendability since determining whether a map is CP and trace-preserving using the Choi representation can be done in much less time than an SDP.

When applied to our problem at hand, this procedure allowed us to test over 540,000 codes in a reasonable amount of time. Specifically, we randomly selected 5000 codes (without constant columns) in all (n, m) classes up to $(20, 10)$, as well as the $(20, 11)$, $(20, 12)$, $(20, 13)$, $(20, 14)$ classes, for a total of 548,818 codes [28]. For each code, we tested symmetric extendability of the state (20) within the gap at $Q = 0.28, 0.29, 0.30, 0.31, 0.32, 0.33$. For approximately 99% of the codes, the special map \mathcal{E} from our procedure gave us a symmetric extension at all QBERs tested. For the remaining codes, the SDP (11) confirmed symmetric extendability for all QBERs tested. In other words, none of the selected codes could break symmetric extendability in the gap.

V. SUMMARY & OUTLOOK

We have examined two-way classical post-processing protocols for PM-based six-state QKD protocols. Specifically, we were interested in determining the existence of such protocols in the gap of Figure 1 for a particular class of states corresponding to Alice and Bob's measurement data. We used the results from Myhr et al. [13] to reduce the problem to breaking symmetric extendability and showed that it is sufficient to consider post-selection by Bob on error-correction codes. Using this framework, we showed that repetition codes achieve the current-best Chau threshold that was previously obtained using the advantage distillation protocol, and we performed an exhaustive search over inequivalent codes of small block lengths and number of codewords and observed that the repetition code has the highest updated threshold for each block length. In particular, for fixed block length, we found that increasing the number of codewords tends

to decrease the threshold. We then considered the less general case of post-selection by Alice on the same code as Bob. We found that the simplex codes, a generalization of repetition codes to more than two codewords, also achieve the Chau threshold. As well, from a random search on over 540,000 codes of larger block lengths and number of codewords, we found that none of the codes broke symmetric extendability in the gap. Notably, our special map \mathcal{E} was able to construct a symmetric extension throughout the gap for approximately 99% of the codes tested.

Based on our results, we conjecture that repetition codes are optimal for each block length and therefore that the Chau threshold is an upper bound on PM-based six-state QKD protocols with two-way classical post-processing. This is in contrast to the entanglement-based version of such protocols in which secret key can be distilled right up to the entanglement limit of $Q = \frac{1}{3}$ by allowing Alice and Bob to first perform *quantum* post-processing (e.g., entanglement distillation, quantum privacy amplification [29–32]) before measuring their systems. As mentioned in the introduction, if repetition codes are indeed optimal, then it would also settle the question of the existence of the separation between secrecy formation and secrecy extraction and of the existence of bound secrecy. We thus hope that our results can guide any future attempts at a proof of the optimality of repetition codes.

ACKNOWLEDGMENTS

We thank the NSERC Discovery Grant and Industry Canada for financial support. SK also acknowledges financial support from the NSERC Canada Graduate Scholarship and the Ontario Graduate Scholarship.

-
- [1] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).
 - [2] See [5] for an introduction to symmetrically extendable states. See [27, 33] for the only currently-known necessary and sufficient criteria for symmetric extendability that hold for two classes of states. From now on, by symmetrically extendable we will always mean symmetrically extendable to a copy of Bob's system.
 - [3] T. Moroder, M. Curty, and N. Lütkenhaus, Phys. Rev. A **74**, 052301 (2006).
 - [4] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).
 - [5] G. O. Myhr, *Symmetric Extension of Bipartite Quantum States and its Use in Quantum Key Distribution with Two-Way Postprocessing*, Ph.D. thesis, Friedrich-Alexander-Universität Erlangen-Nürnberg (2010).
 - [6] D. Gottesman and H.-K. Lo, IEEE Transactions on Information Theory **49**, 457 (2003).
 - [7] H. F. Chau, Phys. Rev. A **66**, 060302 (2002).
 - [8] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (1984) pp. 175–179.
 - [9] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
 - [10] U. M. Maurer, IEEE Transactions on Information Theory **39**, 733 (1993).
 - [11] A. Acín, J. Bae, E. Bagan, M. Baig, L. Masanes, and R. Muñoz Tapia, Phys. Rev. A **73**, 012327 (2006).
 - [12] J. Bae and A. Acín, Phys. Rev. A **75**, 012334 (2007).
 - [13] G. O. Myhr, J. M. Renes, A. C. Doherty, and N. Lütkenhaus, Phys. Rev. A **79**, 042329 (2009).
 - [14] A. Acín and N. Gisin, Phys. Rev. Lett. **94**, 020501 (2005).
 - [15] N. Gisin and S. Wolf, “Linking classical and quantum key agreement: Is there “bound information”?” in *Advances in Cryptology — CRYPTO 2000: 20th Annual International Cryptology Conference Santa Barbara, California, USA, August 20–24, 2000 Proceedings*, edited by M. Bellare (Springer Berlin Heidelberg, Berlin, Heidelberg, 2000) pp. 482–500.
 - [16] N. Gisin, R. Renner, and S. Wolf, “Bound information: The classical analog to bound quantum entangle-

- men,” in *European Congress of Mathematics: Barcelona, July 10–14, 2000 Volume II*, edited by C. Casacuberta, R. M. Miró-Roig, J. Verdera, and S. Xambó-Descamps (Birkhäuser Basel, Basel, 2001) pp. 439–447.
- [17] Gisin, Renner, and Wolf, *Algorithmica* **34**, 389 (2002).
- [18] D. Collins and S. Popescu, *Phys. Rev. A* **65**, 032321 (2002).
- [19] R. Renner and S. Wolf, in *Advances in Cryptology — EUROCRYPT 2003*, Lecture Notes in Computer Science, Vol. 2656, edited by E. Biham (Springer-Verlag, 2003) pp. 562–577.
- [20] N. Lütkenhaus, in *Quantum Information and Coherence*, edited by E. Andersson and P. Öhberg (Springer, 2014) Chap. 10, pp. 107–146.
- [21] Normalization of the state is unimportant for symmetric extendability since if ρ^{AB} is symmetrically extendable then so is $\alpha\rho^{AB}$ for any $\alpha > 0$.
- [22] S. Khatri, *Symmetric Extendability of Quantum States and the Extreme Limits of Quantum Key Distribution*, Master’s thesis, University of Waterloo (2016).
- [23] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes* (North-Holland Publishing Company, 1977).
- [24] J. Lofberg, in *Computer Aided Control Systems Design, 2004 IEEE International Symposium on* (2004) pp. 284–289.
- [25] B. O’Donoghue, E. Chu, N. Parikh, and S. Boyd, *Journal of Optimization Theory and Applications* **169**, 1042 (2016).
- [26] J. Watrous, “Theory of quantum information,” (2016).
- [27] K. S. Ranade, *Journal of Physics A: Mathematical and Theoretical* **42**, 425302 (2009).
- [28] Not all of the codes selected initially were inequivalent. The total number of tested codes given is the number of inequivalent codes based on determining the equivalence of codes according to the results of the procedure described above. See [22] for details.
- [29] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, *Phys. Rev. Lett.* **76**, 722 (1996).
- [30] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, *Phys. Rev. A* **54**, 3824 (1996).
- [31] C. Bennett and G. Brassard, *IBM Technical Disclosure Bulletin* **28**, 3153 (1985).
- [32] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, *Phys. Rev. Lett.* **77**, 2818 (1996).
- [33] J. Chen, Z. Ji, D. Kribs, N. Lütkenhaus, and B. Zeng, *Phys. Rev. A* **90**, 032318 (2014).

Appendix A: Repetition Code Thresholds

In this section, we provide a sketch of the proof that the solution to Eqn. (9) gives the repetition code thresholds $Q_{\mathcal{R}_n}^*$. This proof also establishes the fact that the thresholds with and without post-selection by Alice on repetition codes are the same. For all the details, see [22].

We start with the state in Eqn. (20) for the case when Alice and Bob post-select on the repetition code \mathcal{R}_n :

$$(K_{\mathcal{R}_n} \otimes K_{\mathcal{R}_n})(\rho_Q^{AB})^{\otimes n}(K_{\mathcal{R}_n} \otimes K_{\mathcal{R}_n})^\dagger. \quad (\text{A1})$$

This is a two-qubit state, and it is known from [33] that any two-qubit state ρ^{AB} is symmetrically extendable if and only if

$$\text{Tr}[(\rho^B)^2] \geq \text{Tr}[(\rho^{AB})^2] - 4\sqrt{\det(\rho^{AB})}, \quad (\text{A2})$$

where $\rho^B = \text{Tr}_A[\rho^{AB}]$. By substituting the state (A1) into (A2) and simplifying, we obtain

$$4Q^{2n} - 4Q^n(1 - Q)^n + (1 - 2Q)^{2n} \leq 0. \quad (\text{A3})$$

At equality, this is Eqn. (9) and its solution gives the symmetric extendability thresholds of the state (A1) with post-selection by Alice, while we are interested in the symmetric extendability thresholds of the state (1) *without* post-selection by Alice. Remarkably, by applying the special procedure of Section IV B to the state $\rho_{Q, \mathcal{R}_n}^{A\tilde{B}}$ without post-selection by Alice, we get that the map \mathcal{N} is completely-positive and trace-preserving whenever the condition (A3) is satisfied. In other words, if the state (A1) is symmetrically extendable, then so is $\rho_{Q, \mathcal{R}_n}^{A\tilde{B}}$. Since the converse of this statement is true, it holds that $\rho_{Q, \mathcal{R}_n}^{A\tilde{B}}$ is symmetrically extendable if and only if (A1) is symmetrically extendable. This means that the solution to Eqn. (9) gives the threshold $Q_{\mathcal{R}_n}^*$ and therefore that the thresholds with and without post-selection by Alice are the same for repetition codes. Whether there exist other classes of codes, in addition to the repetition codes, for which the thresholds are the same is an open problem.

Appendix B: Thresholds With and Without Post-Selection by Alice

In [22], we determined for each of the inequivalent codes tested in Section III the corresponding threshold for the states (20) with post-selection by Alice on the same code as Bob. For the vast majority of these codes, the difference between the two thresholds was on the order of 10^{-4} or less. (Recall from Section III B that our procedure for determining the threshold is accurate to within 8.5×10^{-4} .) For some codes, however, the difference was higher. Table II shows some of the codes with the highest difference. The smallest difference is 1.5×10^{-3} and the largest difference is 6.8×10^{-3} . These differences are only marginally greater than the 8.5×10^{-4} within which the thresholds themselves are accurate. A more refined analysis should therefore be performed to confirm the differences seen here. For example, one can take a small interval around the thresholds given in the table and perform the same procedure described in Section III B. The number of points in the interval should be large enough so that the spacing between points is smaller than 8.5×10^{-4} and thus the accuracy of the threshold is higher.

Note also that all of the codes in Table II are non-linear. In fact, for all the inequivalent linear codes tested (which, apart from the two-codeword repetition codes,

$\begin{bmatrix} 000 \\ 100 \\ 110 \\ 111 \end{bmatrix}$	0.1965	$\begin{bmatrix} 0000 \\ 1000 \\ 1110 \\ 1111 \end{bmatrix}$	0.2196
	0.1948		0.2154
$\begin{bmatrix} 0000 \\ 1100 \\ 1110 \\ 1111 \end{bmatrix}$	0.2158	$\begin{bmatrix} 00000 \\ 10000 \\ 11110 \\ 11111 \end{bmatrix}$	0.2330
	0.2143		0.2281
$\begin{bmatrix} 000 \\ 100 \\ 101 \\ 110 \\ 111 \end{bmatrix}$	0.1833	$\begin{bmatrix} 0000 \\ 1000 \\ 1100 \\ 1110 \\ 1111 \end{bmatrix}$	0.2101
	0.1815		0.2043
$\begin{bmatrix} 0000 \\ 1000 \\ 1100 \\ 1101 \\ 1110 \\ 1111 \end{bmatrix}$	0.2004	$\begin{bmatrix} 0000 \\ 1000 \\ 1010 \\ 1100 \\ 1110 \\ 1111 \end{bmatrix}$	0.2021
	0.1962		0.1953

TABLE II. Codes with a large difference between thresholds with and without post-selection by Alice on the same code as Bob. The thresholds are indicated to the right of each code and are accurate to within 8.5×10^{-4} . The top threshold corresponds to the states (1) without post-selection by Alice and the bottom to the states (20) with post-selection by Alice on the same code as Bob.

comprised only four-codeword codes), the difference between the thresholds was on the order of 10^{-5} or less. We also observed the following for the best codes presented in Section III C. Since the thresholds for the best codes in the $m = 2$ and $m = 4$ classes are the repetition code thresholds, as mentioned in Section IV the thresholds with and without post-selection by Alice are equal. For the six best $m = 3$ codes, the threshold difference was on the order of 10^{-5} , for the two best $m = 5$ and $m = 6$ codes on the order of 10^{-8} , and for the single best $m = 7$ code on the order of 10^{-11} .